CSM TACACSとISEの統合

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ネットワーク図</u>
認証手順
<u>ISE の設定</u>
<u>CSMの設定</u>
<u>確認</u>
<u>トラブルシュート</u>

概要

このドキュメントでは、管理者ユーザがTACACS+プロトコルで認証できるように、Cisco Security Manager(CSM)とIdentity Services Engine(ISE)を統合する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Security Manager(CSM)
- Identity Services Engine(ISE).
- TACACSプロトコル。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CSMサーババージョン4.22
- ISE バージョン 3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

デフォルトでは、Cisco Security Manager(CSM)はCiscoworksという認証モードを使用してユー ザをローカルで認証および許可し、中央集中型の認証方式を使用するために、TACACSプロトコ ルを使用してCisco Identity Service Engineを使用できます。

設定

ネットワーク図



認証手順

ステップ1:管理ユーザのクレデンシャルを使用してCSMアプリケーションにログインします。

ステップ2:認証プロセスがトリガーされ、ISEがローカルまたはActive Directoryを介してクレデ ンシャルを検証します。

ステップ3:認証が成功すると、ISEはCSMへのアクセスを許可する許可パケットを送信します。

ステップ4:CSMはユーザ名とローカルユーザロールの割り当てをマッピングします。

ステップ5:ISEは成功した認証のライブログを表示します。

ISE の設定

ステップ1:3回線アイコンを選択します 左上に表示され、[Administration] > [Network Resources] > [Network Devices]に移動します。

Claco ISE		Administration - Network Resources								
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services			
Network Devices Default Device	Network	k Devices								
Device Security Settings	/ tax + A	dd 🚺 Duplicate 🕁 Import	쇼 Export ~ 음 Generate PA	0 🔋 Delete 🗸						
	Name	e 🗠 IP/Mask Profile P	Name Location	Туре	Description					

ステップ2:+Addボタンを選択して、Network Access Device NameとIP Addressに適切な値を入力 し、次に**TACACS Authentication Settingsチェックボックスを確認し、共有秘密を定義**します。「 送信」ボタン**を選択**します。

NEWOX SERVES	anna bende broge melana bende muines exemis noundo aerres noundo aerres anguendes nou meragers exemis muin badason aerres
National Devices	Nestervit Denices List > Row Research Denice
Default Device Device Security Settings	Network Devices * Name COM422 Description
	E PARH v *P: 1025243.42 / 32 0v
	* Device Profile
	Wood Name
	Butware Wrister
	Lesston All Locations v Set 7s Default 1950 In 1950 Device v Set 7s Default
	Device fulle All Device Types v Set Te Default
	KADUS Authentication Settings XADACS Authentication Settings
	David Social American Section
	Lease any Control New O Lease Control New TRACE Shall Compliance Single Control Support
	□ ✓ SNMP Settings
	Advanced Trustsec Settings
	Buteral Cancel
	—
— —! = =	

ステップ3:3つの回線アイコンを選択します [Identity Management] > [Groups**]に移動します**。 左上隅に表示され、[Administration] >

E Cisco ISE		Administration · Identity Ma	anagement
dentities Groups External Ide	ntity Sources	Identity Source Sequences	Settings
Identity Groups	User	Identity Groups	
> 🗅 Endpoint Identity Groups	🖉 Edit	+ Add 🍵 Delete 🗸 🕁 Import	t 🏠 Export 🖂
> 🗖 User Identity Groups		Name	∧ Description
		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
		M Employee	Default Employee User Group
		SROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
		SuestType_Contractor (default)	Identity group mirroring the guest type
		F GuestType_Daily (default)	Identity group mirroring the guest type
		Number 2018 SocialLogin (default)	Identity group mirroring the guest type
		Number 2 Substructure (State	Identity group mirroring the guest type
	0	SOWN ACCOUNTS (default)	Default OWAL ACCOUNTS (default) Liter Group

ステップ4:[User Identity Groups]フォ**ルダに移動**し、[**+Add**]ボタン**を選択**します。名前を定義し、 「送信」ボタン**を選択**します。

lentities Grou	ps External Ide	entity Sources	Identity Source Sequences Settings	
Identity Groups		User Ic	entity Groups	
< 12	0			Selected 0 Total 10 📿
> 🗖 Endpoint	Identity Groups	0 Edit +	udd 🎁 Delete 🗸 🕁 Import 🛧 Export 🗸	All 🗸
> 🛅 User Ide	> 🛅 User Identity Groups	Nar	ne ^ Description	
		0 4	LL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
		- *	SM Admin	
		0 #	ISM Oper	

注:この例では、CSM AdminおよびCSM Oper Identityグループを作成します。CSMの管理 ユーザのタイプごとに、ステップ4を繰り返すことができます

ステップ5:3回線アイコンを選択します [Administration] > [Identity Management] > [Identities]に移動します。[+Add]ボタンを選択し、ユーザ名とパスワードを定義してから、ユーザが属するグループを選択します。この例では、csmadminユーザとcsmoperユーザを作成し、それぞれCSM AdminおよびCSM Operグループに割り当てます。

entities Groups Ex	ternal identity Sources Identity Source Sequences Settings	
	Newark Access Usam Usar > cenodras	
Neral Norman Scan Heb	V Network Access User	
	ious Content v	
	[nal	
	~ Passwords	
	Passand type: Internal blans. V	
	Password Re-Street Password	
	*Lopi Fasword	0
		0
	V User Information	
	Frankana	
	Last Name	
	V Account Options	
	Description	
	Charge paesward on hod togs.	
	V Account Disable Policy	
	Disable account if data anceeds 2021-36-36 (systemet-dd)	
	V User Bround	
	- 1001 010000	
	E CSM Admin v - +	

Identities	Groups	External Identity Sources	Identity Source Sequences	Settings			
Users Latest Manual Netv	work Scan Res	Network A	ccess Users				
						Selected 0 Total 2 🧲	•
		Edit + Add	🛠 Change Status 🗸 🕁 Import	🟦 Export 🗸 🧯 Delete 🗸	Duplicate	All V	V
		Status	Name Descript	tion First Name Last Na	ame Email Address	User Identity Grou Ad	
		Enabled	1 csmadmin			CSM Admin	
		Enabled	2 csmoper			CSM Oper	

ステップ6:選択 [Administration] > [System] > [Deployment]に移動します。ホスト名ノー ドを選択し、デバイス管理サービ**スを有効にします**

Deployment	0	Deployment Nodes				
> 🔆 Deployment		🖉 Edit 🛞 Register 🏷 Syncup 🔒 Deregister		Selected 0	All V	» 7
age PAN Fallover		🗌 Hostname 🥎 Personas	Role(s)	Services	Node Status	
		Les30 Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE		
		Enable SXP Ser Enable Device Admin Service Enable Passive Identity Servi	vice i	(

注:分散導入の場合は、TACACS要求を処理するPSNノードを選択します

ステップ7:3つの回線アイコンを選択し、[Administration] > [Device Administration] > [Policy Elements]に移動します。[Results] > [TACACS Command Sets]に移動します。[+ Add]ボタンを選択して、コマンドセットの名前を定義し、[Permit any command that is not listed below]チェックボックスをオンにします。Submit を選択します。

E Cisco ISE			Work Centers -	Device Administration		Evaluation Mod	e 39 Days Q 💿	53	¢
Overview Identitie	s	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More \sim		
onditions	>	TACACS Command Sets Command Set	> New						
etwork Conditions	>	Mama							
esults	~	Permit all							
Allowed Protocols									
TACACS Command Sets		Description							
TACACS Profiles				i.					
		Commands							
		Permit any command that	t is not listed below	0					
		+ Add 🛛 Trash 🗸	🖉 Edit 🔿 Move Uj	p 💛 Move Down					
		Grant	Command	Arguments					
		No data found.							
							Canad		

ステップ8: 左上の3つの回線アイコンを選択し、[Administration] > [Device Administration] >

[Device Admin Policy Sets]に移動します。選択 (Policy Sets title]の下にある名前を定義し、 中央の[+]ボタンを選択して新しい条件を追加します。

Policy	Sets				Reset Reset Policyse	Hitcounts		Save
۲	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequen	ce Hits	Actions	View
0	Search							
	۲	CSM Administrators		+	Select from list \sim	F	{ĝ}	>
	۲	Default	Tacacs Default policy set		Default Device Admin 🛛 🛇	+ 0	(2)	•

ステップ9:[Condition]ウィンドウで、[add a attribute]を選択し、[**Network Device** Icon]、[Network access device IP address]の順に選択します。 [Attribute **Value]を選択**し、CSM IPアドレスを追加します。[**Use once** done]を選択します。

Conditions Studio					
brary	Editor				~
Search by Name		Network Access-D	evice IP Address		(8)
	Ŗ	Equals 🗸	10.88.243.42		
o conditions found - reset filters.		Set to 'Is not'		Duplicate	Save
			NEW AND OR		
				Glose	Use

ステップ10:[allow protocols]セクションで、[**Device Default Admin**]を選択します。[保存(Save)] を選択します。

Policy Sets				Reset Pol	icyset Hitcounts		Save
Status Policy Set Name	Description	Condition		Allowed Protocols / Server S	equence Hits	Actions	View
Q Search							
CSM 4.22		₽ Netw Addr	Access-Device IP EQUALS 10.88.243.42	Default Device Admin	a ∼+ •	<u>م</u>	•

ステップ11:右矢印を選択します

アイコンをクリックします。

ステップ12:選択 └── [Authentication Policy title]の下にある名前を定義し、中央の[+]を選択して 新しい条件を追加します。[条件]ウィンドウで、[属性の追加]を選択し、[ネットワークデバイスア イコン]を選択し、次に[ネットワークアクセスデバイスのIPアドレス]を選択します。 [Attribute Value]を選択し、CSM IPアドレスを追加します。完了したら[使用]を選択します

ステップ13:IDストアとして[内部ユーザー]を選択し、[保存]を選択します

V Authentication Policy (1)								
Status Rule Name Cor	ditions	Use	Hits	Actions				
Q Search								
		Internal Users 🛛 🗵 🗸						
CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	> Options		{ĝ}				

注:ISEがActive Directoryに参加している場合、IDストアをADストアに変更できます。

ステップ14:選択 認可ポリシーのタイトルの下にある名前を定義し、中央の+ボ**タンを選**択 して新しい条件を追加します。[Condition]ウィンドウで、[add an attribute]を選択し、[**Identity Group**]アイコンを選択し、続いて[Internal User:Identity Group。[CSM Admin Group]を選択し、 [Use]を選択します。

Library	0	Editor				
Search by Name			InternalUser-Identity	Group		0
♥ □ □ ♣ ◎ 및 및 문 ◙ 2 !	0 1 0 t P	45	Equals 🗸	User Identity Groups:CSM Ade	min × 🗸 🗸	ш
EAP-MSCHAPv2	0		Set to 'Is not'		Duplicate	Save
# 📄 EAP-TLS	٥			NEW AND OR		
: Guest_Flow	0					
E Network_Access_Authent	ication_ ()					

ステップ15:[Command Set]で、[Step 7で作成したすべてのコマンドセットを許可]を選択し、 [Save]を選択します

CSM Operグループに対してステップ14と15を繰り返します

 Author 	ization	Policy (3)								
					Results					
⊕ s	Status	Rule Name	Con	ditions	Command Sets		Shell Profiles		Hits	Actions
Q	Search									\supset
	•	CSM Oper	я	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all ×	~+	Select from list	~+	0	{\$}
	0	CSM. Admin	А.	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$\text{Permit all} \times$	~+	Select from list	~+	0	{}
	•	Default			DenyAllCommands ×	\sim +	Deny All Shell Profile	∞ ~+	0	{ô}

ステップ 16(オプション): 左上にある3つの回線アイコンを選択し、[Administration] > [System] > [Maintenance] > [Repository]を選択して、[+Add]を選択し、トラブルシューティングのためにTCPダンプファイルを保存するリポジトリを追加します。

ステップ 17(オプション): リポジトリ名、プロトコル、サーバ名、パス、およびクレデンシャルを定義します。完了したら[**送信**]を選択します。

Deployment	Licensing	Certificates I	Logging	Maintenance	Upgrade	Health Checks	Backup	Click here to do visibility setup Do not show this again.
Patch Management		Repository List > A	Add Repository					
Repository		Repository Co	onfiguration	1				
Operational Data Pur	ging		-					
		* Repository Nam	e VMRepos	itory				
		* Protocol	FTP 🗸					
		Location						
		* Server Name	10.122.1	12.137				
		* Path	1					
		Credentials						
		* User Name	cisco					
		* Password						

CSMの設定

ステップ1 : ローカル管理者アカウントでCisco Security Managerクライアントアプリケーション にログインします。メニューから[Tools] > [Security Manager Administration]に移動します

	E
	Cisco Security Manager Version 4.22.0 Service Pack 1
	Server Name 10.88.243.42 V Username admin Password ••••••
	Default View Configuration Manager
© 2020 Cisco Systems, Inc. Cisco, Cisco Syste its affiliates in the U.S. and certain other coun	erns and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or CISCO tries.



ステップ2:[Native RBAC Parameters]の下のボックス**をオンにします。**[保存して閉じる]を選択し ます

5	Cisco Security Manager - Administration	_ _ ×
API AutoLink ALLALINK ALLALINK ALLALINK ALLALINK ALLALINK ALLALINK ALLALINK COS HADLE COSTAND COSTAND	Derved Security Use the buttons below to cross launch the Server Security Tools within Common Services. AAA Setup Certificate Setup Single Sign On Local User Setup System Identity Setup Native RBAC Parameters W Blow logon for user lds not available in Local User Database	Save Reset Restore Defaults

ステップ3:メニューから[File] > [Submit]を選択します。[File] > [Submit]を選択します。

注:設定変更の場合は、すべての変更を保存する必要があります。これらの変更を送信して 展開する必要があります。

ステップ4:CSM Management UIに移動し、<u>https://<enter_CSM_IP_Addressと入力して</u>Server Administrationを選**択します。**



注:手順4 ~ 7は、ISEで定義されていないすべての管理者のデフォルトロールを定義する 手順を示しています。次の手順はオプションです。

ステップ5:認証モードが**CiscoWorks Local**に設定されていることを確認し、**Online** userIDは CSMで作成されたローカル管理者アカウントです。

Home Server • 1	co Security Manag	jer						admin Logout About Feedback
								17 Apr 2021, 14-11 P
Common Services Auto Refresh	Home	Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021 📀
	Security		Backup			Recent	y Completed Jobs	
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ki	Job Type	Status	Description	Completed At
Authorization Mode	CiecoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1370	SystemCheckUtility SystemCheckUtility	Succeeded	SysCheckTest SysCheckTest	Sat Apr 17 05:01:56 PDT 2021 Fri Apr 16 05:00:58 PDT 2021
Single Sign-on Mode	Standalone	Recent Backup Status	Not found or unable to detect	1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
				1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1300	SystemCheckUsity	Succeeded	SysCheck lest	Tue Apr 13 05:00:54 PDT 2021
				1001.1300	System Check Unity	Succession 1	Syscheck Test	Run Avr 11 05:00:55 PDT 2021
				1001,1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021
								More
	System Tasks		wine Users		Management Tasi			Reports
Local User Setup Mul5-Server Trust Manage Configure Single Sign-On	ument	Number of Online users	1	Schedule Back Check for Soft Check for Dev	up ware Updates los Updates		Permission Rep Log File Status Process Status	bot
AAA Mode Selup		Online User Id(s)	admin Send Message	Collect Server	erformation		System Audit Lo	9

ステップ6:[Server]に移動し、[Single-Server Management]を選択します

ciso	cisco Cisco Security Manager				
Home	Server Software Center				
	Security				
Commo	Single-Server Management				
🗹 Auto R	Multi-Server Trust Management				
	Cisco.com Connection Management				
Authentica	AAA Mode Setup	, i			
Authorizat	Admin	,			
Cingle Cig	Processes				
Single Sig	Backup	2			
	Log Rotation				
	Collect Server information				
	Selftest				
	Notify Users				
	Job Browser				
	Resource Browser				
Local Use	System Preferences				
Multi-Serv	CS Log Configurations				
Configure	DiskWatcher Configuration				
AAA Mode	e Setup II				

ステップ7:[Role Management Setup]を選択し、認証時にすべての管理者ユーザが受け取るデフォ ルトの権限を選択します。この例では、Network Administratorが使用されています。選択したら 、既定として**設定を選択します。**

cisco Security Manager							
Home Server * Software Center *							
Navigator Browser-Server Security mode setup	Role Management Setup	Showing 8 records					
Local User Policy Setup	Roles Description	Default Roles					
Role Management Setup	1. Approver Approver Role						
Certificate Setup	2. Help Desk Help Desk Role						
	3. Network Administrator Network Administrator Role	R					
	4. Network Operator Network Operator Role						
	5. Security Administrator Security Administrator Role						
	6. Security Approver Security Approver Role						
	7. Super Admin Super Admin Role						
	8. System Administrator System Administrator Role						
	Add Edit Delete Copy Export Import Set as default Clear	r default					

ステップ8:[Sever] > [AAA Mode Setup Role]の順に選択し、[**TACACS+**]オプションを選択し、最 後に[change]を選択してISE情報を追加します。



cisco Cisco Security Manager
Home Server Software Center
Authentication Mode Setup
AAA Mode Setup
Select a Type: O ACS O Local RBAC
Current Login Mode: Local Authentication
Available Login Modules
1 Local Authentication
2 Local NT System
3 MS Active Directory
4 RADIUS
5 O TACACS+
Change

ステップ9:ISE Ipアドレスとキーを定義します。オプションで、すべてのローカル認証ユーザを許可するか、ログインに失敗した場合は1人のユーザのみを許可するかを選択できます。この例では、フォールバック方式としてOnly adminユーザが許可されています。[OK]を選択して、変更を保存します。

Login Module Options		
Selected Login Module:	TACACS+	
Description:	Cisco Prime TACACS+ login module	
Server:	10.122.112.4	
Port:	49	
SecondaryServer:		
SecondaryPort:	49	
TertiaryServer:		
TertiaryPort:	49	
Key:		
Debug:	True 🔾 False	
	 Allow all Local Authentication users to fal Authentication login. 	lback to the Local
Login fallback options:	 Only allow the following user(s) to fallbac Authentication login if preceding login fails: 	k to the Local
	admin	(comma separated)
	 Allow no fallbacks to the Local Authentica 	ation login.
		OK Cancel



ステップ10:[Server] > [Single Server Management]を選択し、[Local User Setup]を選択して [add]を選択します。

cisc	Cisco Security Manager	
Home	Server V Software Center V	
Commo	Single-Server Management	
🗹 Auto R	Multi-Server Trust Management	
	Cisco.com Connection Management	i i
Authoritor	AAA Mode Setup	
Autienuca		
Authorizat	Admin	1
Single Sig	Processes	
	Backup	1
	Log Rotation	
	Solfoot	
	Notify Liepre	
	Job Browser	
	Resource Browser	
	System Preferences	
Local Use	CS Log Configurations	
Multi-Serv	DiskWatcher Configuration	
Configure		

cisco Cisco Securit	/ Manager
Home Server * Software Center *	
Navigator	Local User Setup
Browser-Server Security mode setup	Showing 206 rec
Local User Setup Role Management Setup	1. Aaron.Logan 2. Adrian.Lotean
Certificate Setup	3. Adrian.Richards
	5. Aida Agular
	Alanc.Castan Alanc.C
	8. allen spiegel 9. Andrew.OConnor
	10. Anwar Khan 11. armand.smith
	12. Bernard Alaton
	14. Bit.Mason
	15. bill.nash 16. Billy.Vaughan
	17. bpiotnik 18 Brutteur konsen
	CSelect items then take an Import Users Export Users Edit Delete Add Modily My Profile

ステップ11:ステップ5でISEの設定セクションの下に作成した同じユーザ名とパスワードを定義 します。この例ではcsmoperとHelp Deskのタスク許可ロールを使用します。[OK]を選択して、管 理者ユーザを保存します。

ssword:					
			Verify Password:		
nail:					
uthorization Type				5	
elect an option: O Full	Authorization 🔾 En	able Task Au	uthorization C Enable Device Authoriza	tion	
Roles		Device	level Authorization		
Help Desk		Not Ap	oplicable		
Approver					
Network Operator					
Network Administrato	v				
System Administrator	,				
Super Admin					
Security Administrato	r				
Security Approver					
				-	

確認

Cisco Security ManagerクライアントUI

ステップ1:新しいウィンドウブラウザを開き、<u>https://<enter_CSM_IP_Address</u>と入力し、 csmadminのユーザ名とパスワードを使用し、ISE設定セクションのステップ5で作成します。

սիսիս CISCO 10.88.243.42 JavaScript: Enabled User ID: csmadmin Cookies: Password: Enabled Login Help Browser: Supported Version **Cisco Security Manager** Copyright(c) 2006 - 2020 Cisco Systems, Inc. All rights reserved.

試行の成功したログインは、ISE TACACSライブログで確認できます

E Cisco ISE			0	perations • TA	CACS		Evaluation Mode 39 Days	Q	0 78	Φ
Live Logs										
🖉 Refresh 🖞 Export To 🗸						Refresh Show Every 3 seconds V Lat	est 20 records 🗸	Within Last 3	l hours 7 Filter V	~
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	N	etwork D	evic.
×		~	Identity		Authentication Policy	Authorization Policy	ise Node	N	ietwork De	vice N
Apr 17, 2021 02:34:54.1		6	csmadmin	Authentic	CSM 4.22 >> Default		ise30	CS	SM422	
Last Updated: Sat Apr 17 2021	1 09:37:58 0	GMT-0500 (C	entral Daylight T	ime)				Reco	rds Show	n: 1

Cisco Security Managerクライアントアプリケーション

ステップ1:helpdesk adminアカウントを使用して、Cisco Security Managerクライアントアプリケ ーションにログインします。

	8
Cisco Security Manager Version 4.22.0 Service Pack 1	
Server Name 10.88.243.42	
Password ••••••	
Default View Configuration Manager Login Help	
Its affiliates in the U.S. and certain other countries.	

試行の成功したログインは、ISE TACACSライブログで確認できます

e Logs								
						Refresh Every 3 seconds 🗸	Show Latest 20 records 🗸	Within Last 3 hours
🔿 Refresh 🖞 Export To 🗸								⊽ Filter ∨ @
C Refresh ⊥ Expert To ∨ Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	lse Node	∑ Filter ∨ @
C Refresh 🖞 Export To 🗸 Logged Time	Status	Details	Identity Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Vetwork Device

ステップ2:CSMクライアントアプリケーションメニューから[Tools] > [Security Manager Administration]を選択すると、特権がないことを示すエラーメッセージが表示されます。

©		Cisco Sec	urity 1	Manager	- Configu	ration N	fanager - cs	moper Connected to	10.88.243.42			- 0 X
File Edit View Policy Map 1	danage To	ofs Launch Help										ababa
Steven Re Policy Rel	cy Bundle	Device Properties	0	5 🐏 E	1 🔒 🗞 i	6 0				9	Search All Categories	CISCO
Denkes 💽 🗑	Healt	Packet Capture Wizard			Dep	loyment	Henager			Device State		
Piter:rene v	00	Fing TraceBaute and Nilcokup	14			fait 8 😐	Fending 5 0	Pasa: 0		Critical 3 O Warning 3 O Nor	nai 0	
er (de Secondare 2) (de Lecation 2) (de Al	🕒 iù 🙀	Pinteligence								LentUpde	te Time: 17 Apr 2021 00	LILI PM PDT 🗗
	N Pile	Show Containment	-6							Q ₁ : type to Search		
	Dap	Inventory Status	1.00	d Aleta	Connection	State	Deployment	Additional Information	3P Address	Host Donain	Target OS Heraion	Running 05 1
	2 5	Catalyst Summary Info		•		. 0	- G +		199, 134, 215, 3	gebetus umfo-3 unde gev	9.9(2)	9.9(2)40
	9	Apply IPS Update		•		- 0	- G o		199, 129, 210, 2	geliatus varvas 2 unde gor	9.900	9.9(2)40
	2 4	Preview Configuration	-	•		0	Q. 0		199, 129, 210, 9	gebalus volves #Lusting	N 9.900	9.9(2)40
	9	Backup		•	•	0	80		199, 139, 233, 30	gel also uses 12 usla g	iv 9.905	9-9(2)40
	9	Security Manager Diagnestics		•		0	Q. 0		199, 134, 215, 4	qu2atus vash-3-aala.gev	9.900	9.9(2)40
Publics	2 3	Security Manager Administration		•		0	Q. 0		199, 129, 213, 4	op also Creves auto Curp	9.900	8.9(2)40
- no device adected -	9 00	Satus-usefo-Sussia-gev 0	0			0	Q. 0		199, 134, 215, 5	qui atus usrle Junta gev	9.9(2)	8.9(2)40
	9 00	Datus-uswas-2 undergev 0	0	•	•	0	Ø.0		199, 139, 210, 5	quil-stue-uswae-1 usda go	9.9(2)	8.9(2)40

You do not have sufficient privileges to perform this operation. Please contact your system administrator and have them grant you additional privileges. If your AAA mode is ACS, privileges are granted via ACS configuration. If your AAA mode is non-ACS, privileges are granted via "CiscoWorks Homepage > Server > Single-Server Management > Local User Setup". OK	1	Error - Insufficient Privileges
		You do not have sufficient privileges to perform this operation. Please contact your system administrator and have them grant you additional privileges. If your AAA mode is ACS, privileges are granted via ACS configuration. If your AAA mode is non-ACS, privileges are granted via "CiscoWorks Homepage > Server > Single-Server Management > Local User Setup". OK

ステップ3:ステップ1から3をcsmadminアカウントで繰り返し、このユーザーに適切な権限が与 えられていることを確認します。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

ISEのTCPダンプツールによる通信検証

ステップ1:ISEにログインし、左上にある3つの回線アイコンに移動し、[Operations] > [Troubleshoot] > [Diagnostic Tools]を選択します。

ステップ2:[一般ツール]で**[TCPダ**ンプ]を選択し、[Add+]を選択します。[Hostname]、[Network Interface File Name]、[Repository]を選択し、オプションでCSM IPアドレス通信フローのみを収 集するフィルタを選択します。[保存して**実行]を選択します**

Cisco ISE

Operations · Troubleshoot

Diagnostic Tools Down	load Logs Debug Wizard
General Tools ~ RADIUS Authentication TroubL Execute Network Device Com	Add TCP Dump Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear. Host Name *
Evaluate Configuration Validat Posture Troubleshooting Agentiess Posture Troublesho EndPoint Debug	ise30 V Network Interface * GigabitEthernet 0 V
TCP Dump	
Session Trace Tests	Filter ip host 10.88.243.42
TrustSec Tools	
	E.g: lp host 10.77.122.123 and not 10.177.122.119 File Name CSM_Tshoot
	Repository VMRepository V
	100 O Mb
	Limit to 1 File(s) 0
	5 O Minute(s)
	Promiscuous Mode Cancel Save and Run

ステップ3:CSMクライアントアプリケーションまたはクライアントUIにログインし、管理者クレ デンシャルを入力します。

ステップ4:ISEで[Stop]ボタンを選択し、pcapファイルが定義されたリポジトリに送信されたことを確認します。

C Re	C Refresh + Add C Edit		📋 Trash 🗸 🕨 Start	\bigcirc Stop $\ \pm$ Download			$\nabla \mathbf{r}$	Filter 🗸 🐵
	Host Name		Network Interface	Filter	File Name	Repository	File S	Number o
	ise30.ciscoise.lab		GigabitEthernet 0	ip host 10.88.243.42	CSM_Tshoot	VMReposit	100	1

File Commands Tools Favorites Options Help Add Extract To Test View Delete Find Vizard Info VisusScan Comment SFX	SM_	Tshoot.zip (on	nly 20 days left to b	uy a licens	e)				_		-	ī
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX	File Con	mmands Too	ols Favorites O	ptions H	elp							
↑ Image: CSM_Tshoot.zip - ZIP archive, unpacked size 1,166 bytes Name Size Packed Type Modified CRC32 Image: File folder File folder	Add	Extract To	Test View	Delete	Q Find	Wizard	info Vit	o 🗐 rusScan Commer	nt	SFX		
Name Size Packed Type Modified CRC32	↑ [💶 CSM_Tsho	oot.zip - ZIP archiv	e, unpacke	d size 1,166 b	ytes						
File folder	Name	^	Size	Packed	Туре		Modified	CRC32				Ī
					File folder							
CSM_Tshoot.pcap 1,166 556 PCAP File 4/17/2021 3:29 8A27888D	CSM_T	lshoot.pcap	1,166	556	PCAP File		4/17/2021 3:29	8A27888D				

ステップ5:pcapファイルを開き、CSMとISE間の正常な通信を検証します。

•••	•				CSM_Tshoot.pcap	
	1	S 🕺 🗋 🔲	् 🗣 👄 警	Ŧ 🗶 🗔	📃 Q, Q, Q, 🎹	
Apply	, a display filter	.<\#/>			Expressi	in +
No.	Time	Source	Destination	Protocol	Length Info	
C.	1 0.000000	10.88.243.42	10.122.112.4	TCP	66 55740 - 49 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1300 WS=256 SACK_PERM=1	
	2 0.000130	10.122.112.4	10.88.243.42	TCP	66 49 - 55740 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128	ł
	3 0.065680	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=1 Ack=1 Win=66048 Len=0	
	4 0.101272	10.88.243.42	10.122.112.4	TACACS+	97 Q: Authentication	
	5 0.101362	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0	
	6 0.107185	10.122.112.4	10.88.243.42	TACACS+	81 R: Authentication	
	7 0.203012	10.88.243.42	10.122.112.4	TCP	60 55740 - 49 [ACK] Seq=44 Ack=28 Win=66048 Len=0	
	8 0.220350	10.88.243.42	10.122.112.4	TACACS+	80 Q: Authentication	
	9 0.209903	10.122.112.4	10.00.243.42	TACACC	34 49 → 30/40 [ALK] 360=28 ACK=70 Win=29312 Len=0	
	10 0.311130	10.122.112.4	10.00.243.42	TER	72 N: Automatication	
	2 8.375973	10.88.243.42	10.122.112.4	TCP	60 55740 - 49 [A(K) Seq=70 Ark=47 Win=66048 Len=0	
	3 8,488651	18,88,243,42	10,122,112,4	TCP	68 55748 + 49 [FIN ACK] Secura Acka7 Wine66048 Lense	
. 1	14 8,488724	18,122,112,4	10.88.243.42	TCP	54 49 - 55748 [A(K] Sec=47 Ack=71 Win=29312 Len=8	
> Fran	ne 6: 81 bytes	on wire (648 bits)	, 81 bytes captured (6	48 bits)		
Ethe	ernet II, Src:	Vmware_a4:0d:c6 (04	0:50:56:a4:0d:c6), Dst	: Cisco_1f:21:4	45 (00:14:6a:1f:21:45)	
> Inte	ernet Protocol	Version 4, Src: 10.	.122.112.4, Dst: 10.88	.243.42		
> Tran	smission Cont NCS+	rol Protocol, Src Po	ort: 49, Dst Port: 557	40, Seq: 1, Ac	k: 44, Len: 27	
M	ajor version:	TACACS+				
м	inor version:	0				
т	ype: Authentic	cation (1)				
5	equence number	r: 2				
> F	lags: 0x00 (Er	ncrypted payload, Mu	<pre>iltiple Connections)</pre>			
S	ession ID: 38	19957939				
8888	00 14 6a 1f 2	21 45 00 50 56 a4 0	d c6 88 88 45 88 ···	1 · ! E · P V · · · · · E	E.	
07	CSM_Tshoot.pca	0			Packets: 14 - Displayed: 14 (100.0%) Prof	le: Default
-						

pcapファイルにエントリが表示されない場合は、次の点を検証します。

- 1. ISEノードでデバイス管理サービスが有効になっている
- 2. CSM設定に正しいISE IPアドレスが追加されている
- 3. ファイアウォールが中央にある場合は、ポート49(TACACS)が許可されていることを確認し ます。